



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/581,359	06/09/2000	CHRISTIAN MENZEL	P00.0622	7112

7590 09/20/2005

Kevin R. Spivak
Morrison & Foerster LLP
2000 Pennsylvania Avenue, N.W.
Washington,, DC 20006-1888

EXAMINER

GURSHMAN, GRIGORY

ART UNIT PAPER NUMBER

2132

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/581,359

Applicant(s)

MENZEL ET AL.

Examiner

Grigory Gurshman

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 September 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. The rejection of claims under 35 USC § 112 has been withdrawn in view of Applicant's amendment of claims 1, 4, 6 and 12.
2. Applicant's amendment of the instant claims merely reflects corrections of grammar.
3. Applicant continues to argue that Szabo and Diffie cannot be combined since Szabo ⁶⁸teaches IMSI while Diffie uses SIM card. In response to applicant's argument that Szabo and Diffie is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Diffie, discloses a method for privacy and authentication in wireless networks (see abstract) and Szabo teaches the device comprising a subscriber data base (ID) and means (MM) for checking whether a transmitted subscriber identification (IMSI) authorizes a subscriber to access the radio system (PRS) – see abstract.
4. Applicant further argues that Examiner's reasoning for combining Diffie with Szabo is a hindsight reconstruction. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge

which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). In this case, one of ordinary skill in the art would have been motivated to modify the system for encryption of information for radio transmission and for authentication of subscribers by authenticating subscribers via subscriber identity mobile cards as taught in Szabo for accessing the radio network of the user group (see Szabo, column 1, lines 60-65).

5. In view of the reasons provided herein, the rejections of claims 1-15 are maintained (see Claim Rejections below).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1- 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie (U.S. Patent No. 5,371,194) in view of Szabo (U.S. Patent No. 6,014,563) .

8. Referring to the instant claims Diffie, discloses a method for privacy and authentication in wireless networks (see abstract).

Diffie teaches providing a secure wireless communication link between a mobile nomadic device and a base computing unit. A mobile sends a host certificate to the base along with a randomly chosen challenge value (CH1) and a list of supported shared key algorithms ("SKCS"). The base determines if the host certificate is valid. If the it is not valid, then the base unit rejects the connection attempt. The base then sends a random number (RN1) encrypted in mobile's public key and an identifier for the chosen SKCS to the mobile. The base saves the RN1 value and adds the CH1 value and the chosen SKCS to messages sent to the base. The mobile unit then validates the the certificate and if the certificate is valid, the mobile verifies under the public key of the base the signature on the message. The signature is verified by taking the base message and appending it to CH1 and the list of shared key algorithms that the mobile provided in the first message. If the base signature is not valid, then the communication attempt is aborted. In the event that the base signature is valid, the mobile determines the value of RN1 by decrypting Pub.sub.-- Mobile, RN1 under the private key of the mobile. The mobile then generates RN2 and the session key, and encrypts RN2 under the Pub.sub.-- Base. The mobile sends the encrypted RN2 and E(Pub.sub.-- Mobile, RN1) to the base. The base then verifies the mobile signature using the Pub.sub.-- Mobile obtained from the Cert.sub.-- Mobile. If the mobile signature is verified, the base decrypts E(Pub.sub.-- Base, RN2) using its private key. The base then determines the session key. The mobile and base may then enter a data transfer phase using encrypted data which is decrypted using the session key which is RN1 .sym.RN2 (see column 1, lines 44-68 through column 2, lines 1-10).

9. Referring to the independent claims 1 and 12, the limitation “communication system comprising an access network ... having authentication equipment” is met by network 30 having authentication equipment in the base unit 27 (see Fig.3). The limitation “allocating a radio channel for the transmission of the information via a radio interface from/to base station of the access network” is met by the communication channel between the base (27) and the network (30) – see Fig.3. The limitation “...mutually transmitting public keys between a mobile station and the base station..” is met by the base station and the mobile unit exchanging the public keys (see Figs. 4b and 4c). The limitation “...encrypting subsequent information to be transmitted ...using one of the public keys received by the base station or the mobile station...” is shown in Figs 4b and 4c. The limitation “...deciphering encrypted information received by the mobile station or base station on the basis of a private key” is met by Fig 5b (block 3 from the top), which shows that base decrypts information received from the mobile station using private key. Diffie, however, does not explicitly teach authenticating the subscriber based on the subscriber identity mobile card.

10. Referring to the instant claims Szabo discloses a radio system for a closed user group (see abstract and Fig.1). Szabo teaches the device comprising a subscriber data base (ID) and means (MM) for checking whether a transmitted subscriber identification (IMSI) authorizes a subscriber to access the radio system (PRS) – see abstract and Fig.1. Szabo teaches that subscribers who belong to the closed user group have an authorization card, on which a subscriber identification IMSI is stored, which authorizes the subscriber to access the radio network. The radiotelephone MS with the card-

reading device conforms to the GSM standard and can thus also be used for the GSM mobile-radio system (see column 2, lines 51-57). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the system for encryption of information for radio transmission and for authentication of subscribers of Diffie by authenticating subscribers via subscriber authorization cards (i.e. identity mobile cards) as taught in Szabo. One of ordinary skill in the art would have been motivated to modify the system for encryption of information for radio transmission and for authentication of subscribers by authenticating subscribers via subscriber identity mobile cards as taught in Szabo for accessing the radio network of the user group (see Szabo, column 1, lines 60-65).

11. Referring to claims 2 – 5, Diffie teaches sending a plurality of keys from the mobile to base and from base to mobile – see SKCS list in Figs. 4a and 4b.

12. Referring to claim 6, Diffie teaches returning an authentication reply by the authentication equipment (see abstract and Fig. 5a).

13. Referring to claim 7, Diffie teaches "checking the subscriber identity by an authentication procedure..." – see Figs. 5a and 5b.

14. Referring to claim 8, Diffie teaches the use of shared (i.e. secret keys) - see abstract.

15. Referring to claims 9 –11, 13 and 14, Diffie shows servicing different networks with plurality of subscribers (see Fig. 3).

16. Referring to claim 15, it is well known in the art to have access network and core networks administered by different operators. For example intranets and VPNs are

Art Unit: 2132

administered by different operators. One of ordinary skill in the art would have been motivated to have access network and core networks administered by different operators for the enhanced security.

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GG
GG

Grigory Gurshman
Examiner
Art Unit 2132


GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100